

**Listing of the Claims:**

1. (Original) A method of improving intrusion detection in a computing network, comprising steps of:

defining intrusion suspicion levels for inbound communications destined for a computing device on the computing network; and

using the defined intrusion suspicion levels to determine if a particular inbound communication destined for the computing device should be treated as an intrusion event.

1 2. (Original) The method according to Claim 1, further comprising steps of:

defining a sensitivity level for filtering intrusion events; and

determining the intrusion suspicion level of the particular inbound communication;

wherein the using step compares the sensitivity level to the determined intrusion suspicion level.

1 3. (Original) The method according to Claim 2, wherein the determining step further  
2 comprises comparing conditions in the computing device to predetermined conditions  
3 which signal a potential intrusion.

1 4. (Original) The method according to Claim 3, wherein the conditions in the  
2 computing device comprise contents of the particular inbound communication.

1 5. (Original) The method according to Claim 4, wherein the conditions in the  
2 computing device further comprise a protocol state of a protocol stack which processes  
3 the particular inbound communication.

1 6. (Original) The method according to Claim 1, further comprising the step of taking  
2 one or more defensive actions when the using step determines that the particular

3 inbound communication should be treated as an intrusion event.

1 7. (Original) The method according to Claim 6, wherein the defensive actions are  
2 determined by consulting intrusion detection policy information.

1 8. (Original) The method according to Claim 6, wherein the intrusion detection  
2 policy information is stored in a network-accessible repository.

1 9. (Original) The method according to Claim 1, wherein the using step further  
2 comprises comparing the particular inbound communication to one or more attack  
3 signatures.

1 10. (Original) The method according to Claim 9, wherein at least one of the attack  
2 signatures is a class signature representing a class of attacks.

1 11. (Original) The method according to Claim 9, wherein the attack signatures are  
2 specified as conditions in intrusion detection rules, and wherein each of the intrusion  
3 detection rules further comprises one or more actions that are to be taken when the  
4 using step determines that the particular inbound communication should be treated as  
5 an intrusion event.

1 12. (Original) The method according to Claim 1, wherein the using step operates in  
2 the computing device for which the particular inbound communication is destined.

1 13. (Original) The method according to Claim 12, wherein the using step operates  
2 within layer-specific intrusion detection logic executing in a protocol stack running on  
3 the computing device.

1 14. (Original) The method according to Claim 1, wherein the using step operates in a  
2 network device which analyzes communications directed to the computing device for

3 which the particular inbound communication is destined.

1 15. (Original) The method according to Claim 1, further comprising steps of:  
2 for each of a plurality of potential intrusion events, defining a set of one or more  
3 conditions which describe the potential intrusion event;  
4 associating a sensitivity level with each of the sets of conditions; and  
5 determining a suspicion level of the particular inbound communication;  
6 wherein the using step determines that the particular inbound communication  
7 should be treated as an intrusion event when conditions pertaining to the particular  
8 inbound communication match a selected one of the sets of conditions and the  
9 determined suspicion level maps to the sensitivity level associated with the selected set  
10 of conditions.

1 16. (Withdrawn) A method for improving intrusion detection in a computing network,  
2 comprising steps of:  
3 classifying an inbound communication destined for a computing device on the  
4 computing network as to an intrusion class which is applicable to the inbound  
5 communication; and  
6 determining whether the applicable intrusion class has one or more associated  
7 intrusion detection policy specifications, and if so, performing actions specified in the  
8 one or more associated intrusion detection policy specifications.

1 17. (Withdrawn) The method according to Claim 16, wherein the actions include  
2 writing a record describing the inbound communication to a file, wherein the record  
3 includes the applicable intrusion class.

1 18. (Withdrawn) The method according to Claim 17, wherein the record includes an  
2 identification of a code element where the inbound communication was processed.

1 19. (Withdrawn) The method according to Claim 18, further comprising the step of:

Serial No. 10/058,689

4

BEST AVAILABLE COPY

2           determining, for each of the records of the file, whether the intrusion class and  
3       identification of the code element identify a specific attack, and if so, creating an  
4       analysis record for the identified specific attack.

1       20. (Withdrawn) The method according to Claim 18, further comprising the step of:  
2           determining, for each of the records of the file, whether the intrusion class and  
3       identification of the code element identify a specific attack, and if not, performing steps  
4       of:

5           locating packet data pertaining to the record;  
6           comparing the located packet data to attack signatures; and  
7           if a matching attack signature is located by the comparing step, creating  
8       an analysis record for a specific attack which corresponds to the matching attack  
9       signature, and otherwise creating an analysis record for the intrusion class.

1       21. (Withdrawn) The method according to Claim 16, wherein the classifying step  
2       further comprises locating an attack signature which matches the inbound  
3       communication, and the determining step further comprises using one or more  
4       keywords which are associated with the located attack signature to retrieve the  
5       associated intrusion detection policy specifications.

1       22. (Original) A system for improving intrusion detection in a computing network,  
2       comprising:  
3           means for defining intrusion suspicion levels for inbound communications  
4       destined for a computing device on the computing network; and  
5           means for using the defined intrusion suspicion levels to determine if a particular  
6       inbound communication destined for the computing device should be treated as an  
7       intrusion event.

1       23. (Original) The system according to Claim 22, further comprising:  
2           means for defining a sensitivity level for filtering intrusion events; and

3       means for determining the intrusion suspicion level of the particular inbound  
4 communication;

5       wherein the means for using the defined intrusion further comprises means for  
6 comparing the sensitivity level to the determined intrusion suspicion level.

1       24. (Original) The system according to Claim 23, wherein the means for determining  
2 further comprises means for comparing conditions in the computing device to  
3 predetermined conditions which signal a potential intrusion.

1       25. (Original) The system according to Claim 22, further comprising means for taking  
2 one or more defensive actions when the means for using determines that the particular  
3 inbound communication should be treated as an intrusion event, wherein the defensive  
4 actions are determined by consulting intrusion detection policy information.

1       26. (Original) The system according to Claim 22, wherein the means for using further  
2 comprises means for comparing the particular inbound communication to one or more  
3 attack signatures, wherein the attack signatures are specified as conditions in intrusion  
4 detection rules, and wherein each of the intrusion detection rules further comprises one  
5 or more actions that are to be taken when the means for using determines that the  
6 particular inbound communication should be treated as an intrusion event.

1       27. (Original) The system according to Claim 22, further comprising:  
2           for each of a plurality of potential intrusion events, means for defining a set of  
3 one or more conditions which describe the potential intrusion event;  
4           means for associating a sensitivity level with each of the sets of conditions; and  
5           means for determining a suspicion level of the particular inbound  
6 communication;  
7           wherein the means for using determines that the particular inbound  
8 communication should be treated as an intrusion event when conditions pertaining to  
9 the particular inbound communication match a selected one of the sets of conditions

10 and the determined suspicion level maps to the sensitivity level associated with the  
11 selected set of conditions.

1 28. (Withdrawn) A system for improving intrusion detection in a computing network,  
2 comprising:

3 means for classifying an inbound communication destined for a computing  
4 device on the computing network as to an intrusion class which is applicable to the  
5 inbound communication; and

6 means for determining whether the applicable intrusion class has one or more  
7 associated intrusion detection policy specifications, and if so, performing actions  
8 specified in the one or more associated intrusion detection policy specifications.

1 29. (Withdrawn) The system according to Claim 28, wherein the actions include  
2 writing a record describing the inbound communication to a file, wherein the record  
3 includes the applicable intrusion class and an identification of a code element where the  
4 inbound communication was processed.

1 30. (Withdrawn) The system according to Claim 29, further comprising:

2 means for determining, for each of the records of the file, whether the intrusion  
3 class and identification of the code element identify a specific attack, and if so, creating  
4 an analysis record for the identified specific attack, and if not, means for:

5 locating packet data pertaining to the record;

6 comparing the located packet data to attack signatures; and

7 if a matching attack signature is located by the means for comparing,  
8 creating an analysis record for a specific attack which corresponds to the matching  
9 attack signature, and otherwise creating an analysis record for the intrusion class.

1 31. (Withdrawn) The system according to Claim 28, wherein the means for  
2 classifying further comprises means for locating an attack signature which matches the  
3 inbound communication, and the means for determining further comprises means for

4       using one or more keywords which are associated with the located attack signature to  
5       retrieve the associated intrusion detection policy specifications.

1       32. (Original) A computer program product for improving intrusion detection in a  
2       computing network, the computer program product embodied on one or more  
3       computer-readable media and comprising:

4              computer-readable program code means for defining intrusion suspicion levels  
5       for inbound communications destined for a computing device on the computing  
6       network; and

7              computer-readable program code means for using the defined intrusion  
8       suspicion levels to determine if a particular inbound communication destined for the  
9       computing device should be treated as an intrusion event.

1       33. (Original) The computer program product according to Claim 32, further  
2       comprising:

3              computer-readable program code means for defining a sensitivity level for  
4       filtering intrusion events; and

5              computer-readable program code means for determining the intrusion suspicion  
6       level of the particular inbound communication;

7              wherein the computer-readable program code means for using compares the  
8       sensitivity level to the determined intrusion suspicion level.

1       34. (Original) The computer program product according to Claim 33, wherein the  
2       computer-readable program code means for determining further comprises computer-  
3       readable program code means for comparing conditions in the computing device to  
4       predetermined conditions which signal a potential intrusion, the conditions in the  
5       computing device comprising contents of the particular inbound communication.

1       35. (Original) The computer program product according to Claim 33, wherein the  
2       computer-readable program code means for determining further comprises computer-

Serial No. 10/058,689

8

BEST AVAILABLE COPY

3        readable program code means for comparing conditions in the computing device to  
4        predetermined conditions which signal a potential intrusion, the conditions in the  
5        computing device comprising contents of the particular inbound communication and a  
6        protocol state of a protocol stack which processes the particular inbound  
7        communication.

1        36. (Original) The computer program product according to Claim 32, further  
2        comprising computer-readable program code means for taking one or more defensive  
3        actions when the computer-readable program code means for using determines that  
4        the particular inbound communication should be treated as an intrusion event, wherein  
5        the defensive actions are determined by consulting intrusion detection policy  
6        information stored in a policy repository.

1        37. (Original) The computer program product according to Claim 1, wherein the  
2        computer-readable program code means for using further comprises computer-  
3        readable program code means for comparing the particular inbound communication to  
4        one or more attack signatures, wherein at least one of the attack signatures is a class  
5        signature representing a class of attacks.

1        38. (Original) The computer program product according to Claim 32, wherein the  
2        computer-readable program code means for using operates in the computing device for  
3        which the particular inbound communication is destined.

1        39. (Original) The computer program product according to Claim 32, wherein the  
2        computer-readable program code means for using operates in a network device which  
3        analyzes communications directed to the computing device for which the particular  
4        inbound communication is destined.

1        40. (Original) The computer program product according to Claim 32, further  
2        comprising:

Serial No. 10/058,689

9

BEST AVAILABLE COPY

3 computer-readable program code means for specifying, for each of a plurality of  
4 potential intrusion events, a set of one or more conditions which describe the potential  
5 intrusion event;

6 computer-readable program code means for associating a sensitivity level with  
7 each of the sets of conditions; and

8 computer-readable program code means for determining a suspicion level of the  
9 particular inbound communication;

10 wherein the computer-readable program code means for using determines that  
11 the particular inbound communication should be treated as an intrusion event when  
12 conditions pertaining to the particular inbound communication match a selected one of  
13 the sets of conditions and the determined suspicion level maps to the sensitivity level  
14 associated with the selected set of conditions.

1 41. (Withdrawn) A computer program product for improving intrusion detection in a  
2 computing network, the computer program product embodied on one or more  
3 computer-readable media and comprising:

4 computer-readable program code means for classifying an inbound  
5 communication destined for a computing device on the computing network as to an  
6 intrusion class which is applicable to the inbound communication; and

7 computer-readable program code means for determining whether the applicable  
8 intrusion class has one or more associated intrusion detection policy specifications, and  
9 if so, performing actions specified in the one or more associated intrusion detection  
10 policy specifications.

1 42. (Withdrawn) The computer program product according to Claim 41, wherein the  
2 actions include writing a record describing the inbound communication to a file, wherein  
3 the record includes the applicable intrusion class and an identification of a code  
4 element where the inbound communication was processed.

1 43. (Withdrawn) The computer program product according to Claim 42, further

Serial No. 10/058,689

10

BEST AVAILABLE COPY

2 comprising:

3 computer-readable program code means for determining, for each of the records  
4 of the file, whether the intrusion class and identification of the code element identify a  
5 specific attack, and if so, computer-readable program code means for creating an  
6 analysis record for the identified specific attack, and if not, computer-readable program  
7 code means for:

8 locating packet data pertaining to the record;

9 comparing the located packet data to attack signatures; and

10 if a matching attack signature is located by the computer-readable  
11 program code means for comparing, creating an analysis record for a specific attack  
12 which corresponds to the matching attack signature, and otherwise creating an analysis  
13 record for the intrusion class.

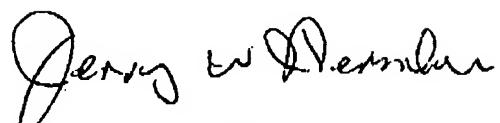
1 44. (Withdrawn) The computer program product according to Claim 41, wherein the  
2 computer-readable program code means for classifying further comprises computer-  
3 readable program code means for locating an attack signature which matches the  
4 inbound communication, and the computer-readable program code means for  
5 determining further comprises computer-readable program code means for using one  
6 or more keywords which are associated with the located attack signature to retrieve the  
7 associated intrusion detection policy specifications.

BEST AVAILABLE COPY

Serial No. 10/058,689

11

Respectfully Submitted,



Jerry W. Herndon

Reg. No. 27,901

IBM Docket No. RSW920020011US1

Serial No. 10/058,689

Customer No. 25259

Phone: 919-543-3754

Fax: 919-254-4330

BEST AVAILABLE COPY

Serial No. 10/058,689

12